Exercise 1: Open Source Information Gathering Using Windows Command Line Utilities

Scenario

**Overview**

As a professional Ethical Hacker or Pen Tester, your first step will be to check for the reachability of a computer in the target network. Operating systems offer several utilities that you can readily use for primary information-gathering. Windows command-line utilities such as ping, nslookup, and tracert gather important information like IP address, maximum Packet Fame size, etc. about a target network or system that form a base for security assessment and pen test.

**Lab Scenario**

As a professional Ethical Hacker or Pen Tester, your first step will be to check for the reachability of a computer in the target network. Operating systems offer several utilities that you can readily use for primary information-gathering. Windows command-line utilities such as ping, nslookup, and tracert gather important information like IP address, maximum Packet Fame size, etc. about a target network or system that form a base for security assessment and pen test.

**Lab Objectives**

This lab demonstrates how to use ping, nslookup, and tracert utilities to gather information about a target. The lab teaches how to:

* Use ping utility to find the IP address of a target domain
* Use ping utility to emulate the tracert (traceroute) command
* Find the maximum frame size for the network

**Lab Duration**: **10** Minutes

1. Click [Windows 10](https://labclient.labondemand.com/Instructions/e6478368-5c22-4747-91f4-d625d7e5866b?rc=10) machine, click [Ctrl+Alt+Delete](https://labclient.labondemand.com/Instructions/e6478368-5c22-4747-91f4-d625d7e5866b?rc=10) link.

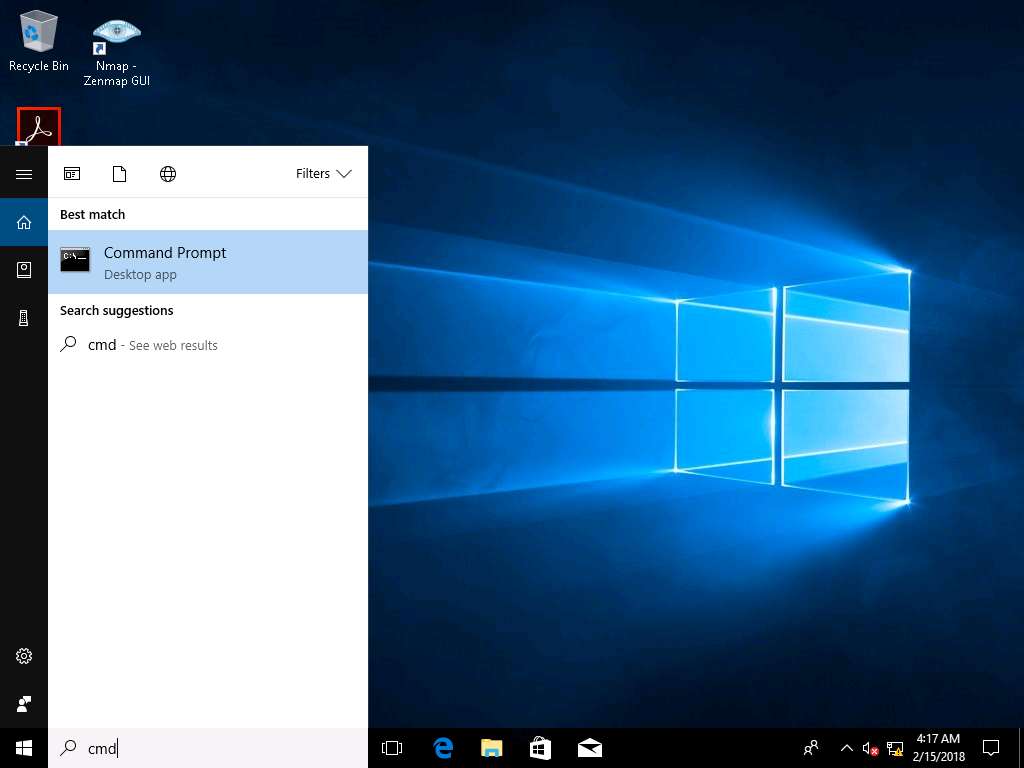


1. By default **Admin** account is selected, click Pa$$w0rd and press **Enter** to login.



1. To launch command prompt, type **cmd** in **Search** field as shown in screenshot, and then click **Command Prompt** from the search result.

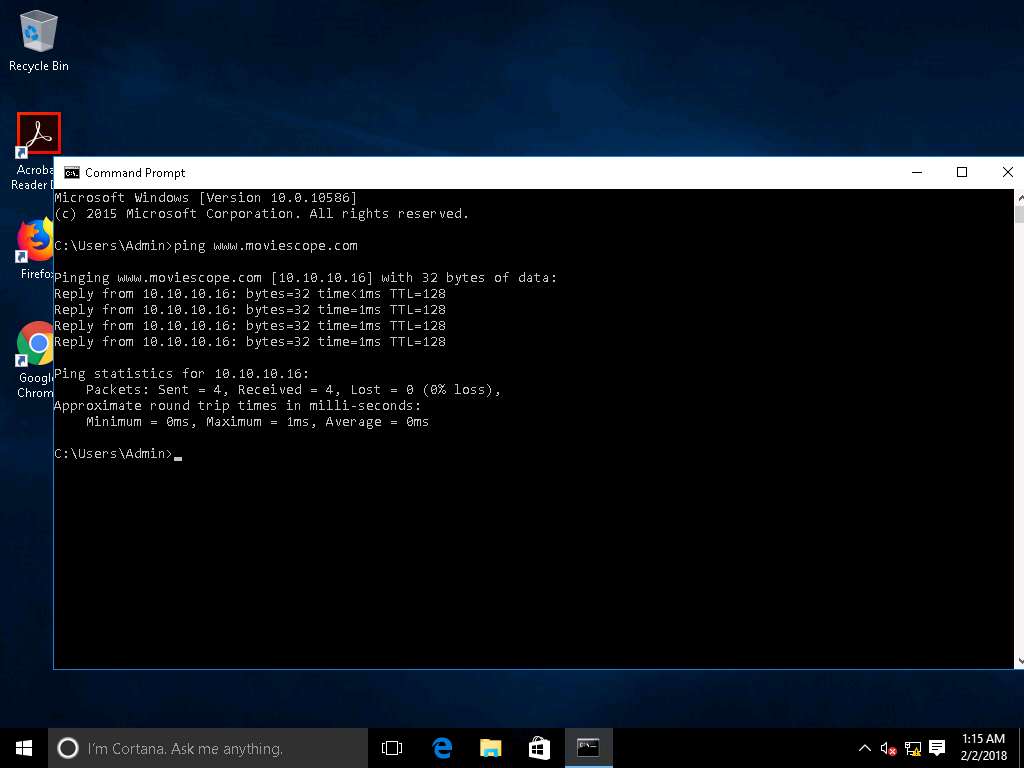
If a **User Account Control** pop-up appears click **Yes**.



1. Type ping **www.moviescopes.com** in the command prompt window, and press **Enter** to find its IP address.

The displayed response should be similar to the one shown in the screenshot.

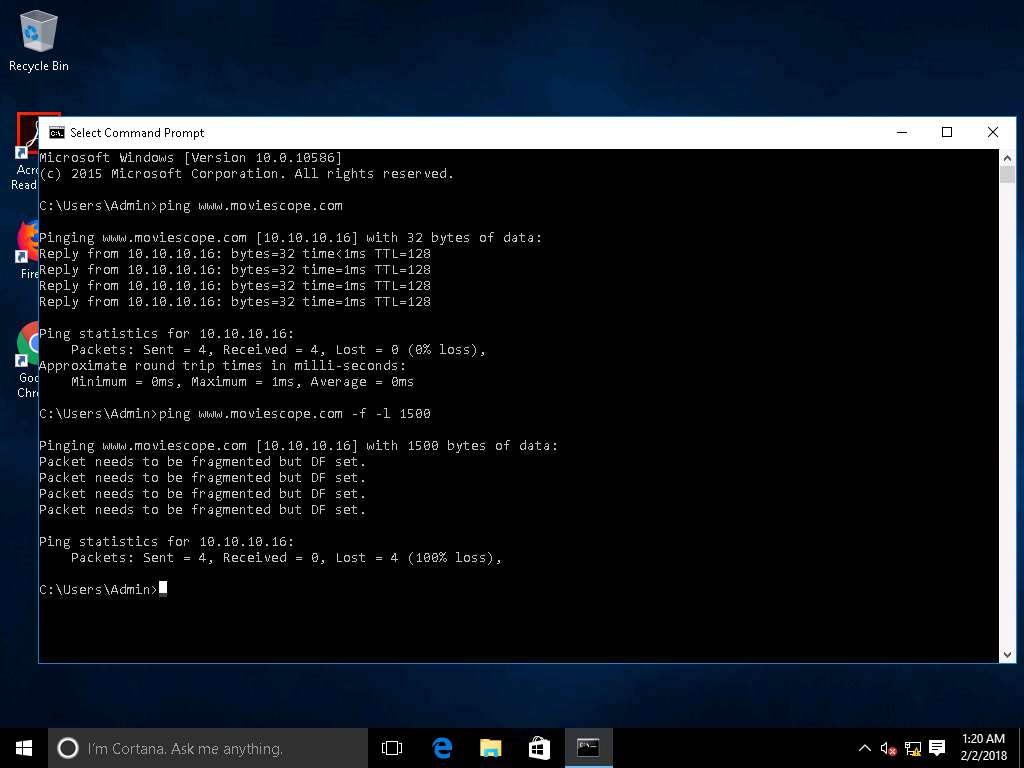
Note the target domain’s IP address in the result above: **10.10.10.16**. (Your result can be different)



1. In the command prompt window, type **ping www.moviescopes.com –f –l 1500** and press **Enter**. The response, **Packet needs to be fragmented but DF set**, means that the frame is too large to be on the network and needs to be fragmented.

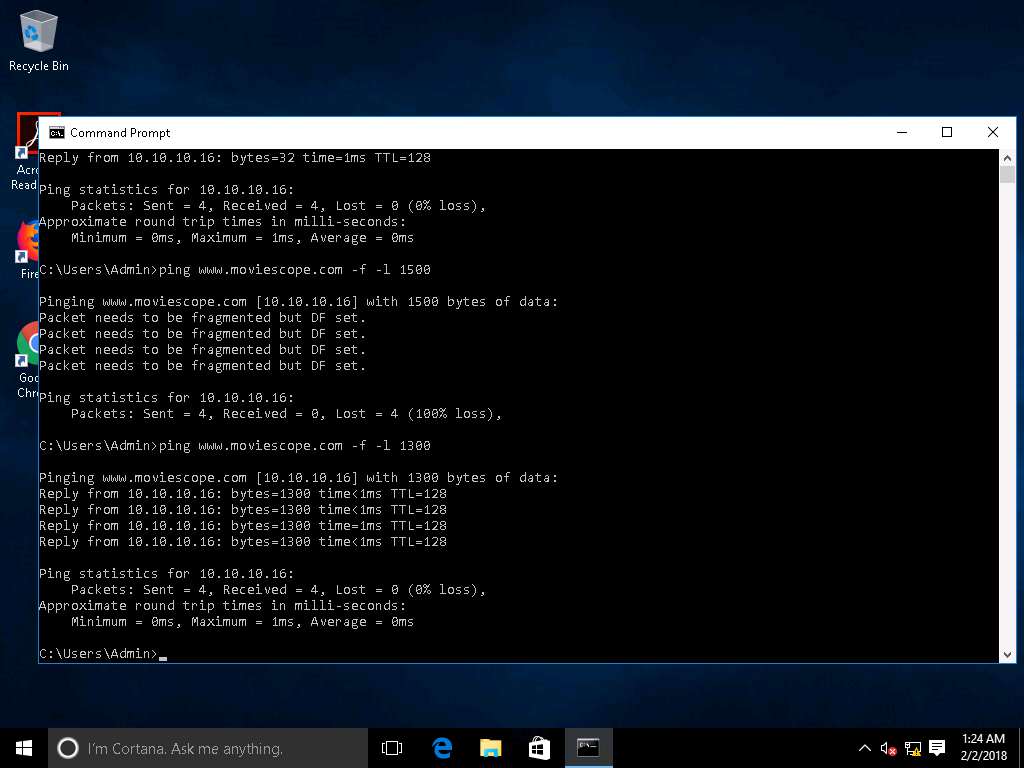
**-f** switch sets the **Do Not Fragment** bit on the ping packet. By default, the ping packet allows fragmentation.

Since we used the **-f** switch with the ping command, the packet was not sent, and the ping command returned this error.

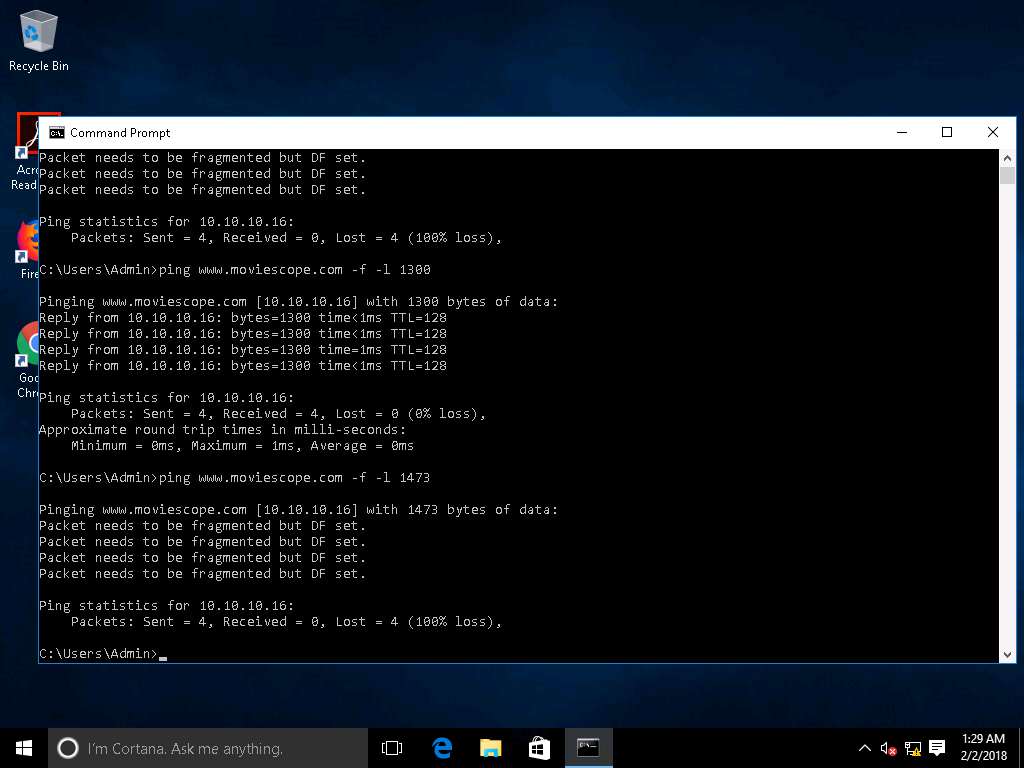


1. Type **ping www.moviescopes.com –f –l 1300** and press **Enter.**

In the ping command, the **–l** option means to send the buffer size.

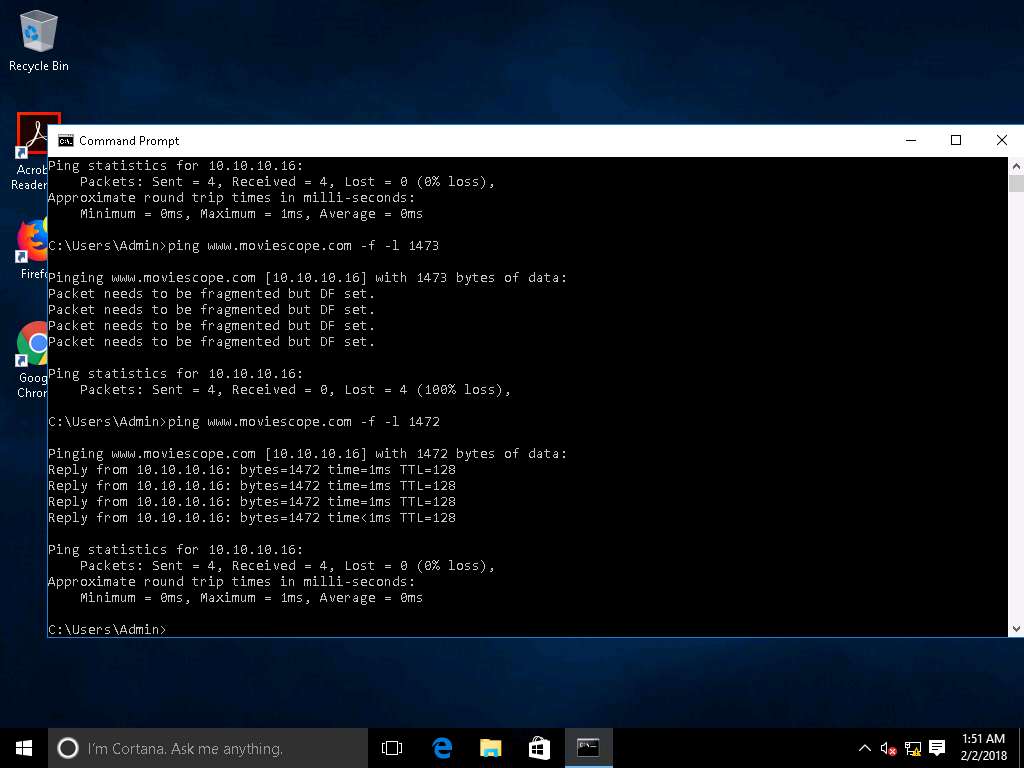


1. Type **ping www.moviescopes.com –f –l 1473** and press **Enter.**  
   The command replies with **Packet needs to be fragmented but DF set.**



1. Type **ping www.moviescopes.com –f –l 1472** and press **Enter.**  
   The command replies with a successful ping.

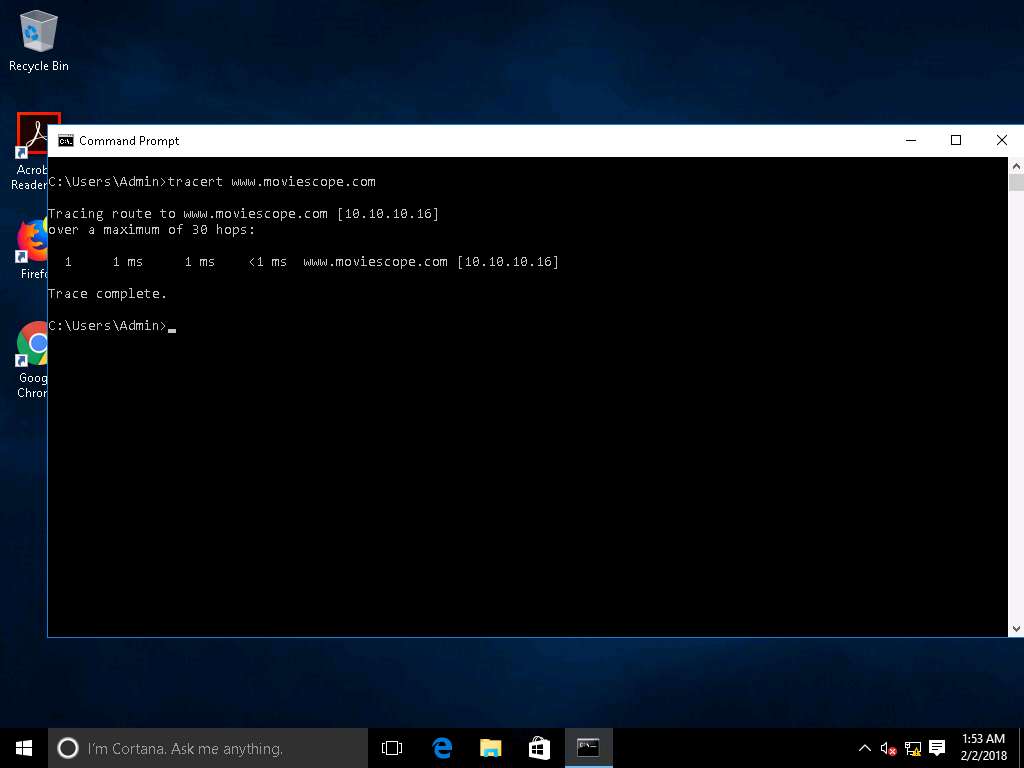
The maximum frame size will differ depending upon on the target network.



1. In the command prompt type **tracert www.moviescopes.com** and press **Enter.**

This command traceroutes the network configuration information of the target domain.

In this lab the command finds the target website in a single hop because it is locally hosted in the Windows Server 2016 machine. (Your results can be different)



In this lab you have learned how to:

* Use ping utility to find the IP address of a target domain
* Use ping utility to emulate the tracert (traceroute) command
* Find the maximum frame size for the network